Information Security Policy: Taxonomy and Development Issues

Lech J. Janczewski, The University of Auckland, Private Bag 92019, Auckland, New Zealand; E-mail: lech@auckland.ac.nz

ABSTRACT

The content of this paper aims at defining what an Information Security Policy (ISP) is, what are the possible ISP formats, and what parts of the ISP are of particular importance. Special emphasis is put on the presentation of methods for the reduction of effort needed for the development of a good ISP.

INTRODUCTION

The answer to the question: *What is an Information Security Policy?* is not so simple. There are many opinions about this, so let's look at what some researchers have considered:

Karen Forch (1994) stated that all organizations should develop a security policy statement and train all employees on its contents. A policy statement should include main checkpoints that are directed specifically at an individual organization's operations including: Avoidance, Deterrence, Prevention, Detection, Recover, and Correction.

DPMA Model Corporate Computer Security Policy Statement (2006) concludes that it is the policy of a company to protect its proprietary information assets and allow the use, access and disclosure of such information only in accordance with corporate interests and applicable laws and regulations.

The Generally Accepted Information Security Principles (GAISP), (2006) draws upon established security guidance and standards to create comprehensive, objective guidance for information security professionals, organizations, governments, and users. The use of existing, accepted documents and standards will ensure a high level of acceptance for the final GAISP product, and will enable a number of benefits to be achieved.

Finally, Ross Anderson (2001) stated:

By security policy I mean a succinct statement of a system's protection strategy (for example, "each credit must be matched by an equal and opposite debit, and all transactions over $1,000 must be authorized by two managers"). A security target is a more detailed specification, which sets out the means by which a security policy will be implemented in a particular product-encryption and digital signature mechanisms, access controls, audit logs, and so on.

The content of this paper summarises a research aimed at defining what an Information Security Policy (ISP) is, what are the possible formats, and what parts of the ISP are of special importance. The content of the paper will therefore include the following parts:

- What is and what is not an ISP,
- What are the possible formats of an ISP,
- Possible approaches used for the development of an ISP
- Important issues regarding the content of an ISP.

The paper terminates with conclusions and suggestions for future research of these issues.

THE BASIC DIFFERENCE

To some extent the authors quoted in the introduction illustrate the basic difference in the approach to what an ISP is. ISP could be a term used for defining:

- Management's point of view about the protection of the information resources of an organization,
- Results of a project aimed on the development of facilities, procedures, and awareness to protect company's information resources,
- Implementation of a project defined above,
- A document distributed to all employees (or to their subset) informing them of information security arrangements.

In this paper we define an ISP as an internal or generally accessible document produced or endorsed by senior management. This document defines policies deployed or to be deployed within the organization to protection the information resources of the organization and that all staff should follow it.

INFORMATION SECURITY POLICY FORMATS

There are many forms of such a document ranging from a one page document, to an extended 200 page long volume. Janczewski & Colarik (2002) defined these basic differences:

- *General ISP*
  This may be a very short document (less than one page) stating that the security of information is of importance for the company, and that all staff are responsible for assuring that data will be accessible only to those authorised, and not changed without authorization. It is an ISP mission statement.
- *Practical ISP*
  This is a collection of basic rules on how to handle company documents and resources to maintain a high level of security. These rules are top level concepts of security do's and don'ts. For instance, it could contain a statement that all the company files need to have backups performed at the end of each working day, or that no staff member is allowed to disclose their password to anyone. A practical ISP is usually a few pages long. This document is presented to every employee and they are asked to sign an acknowledgement.
- *Detailed ISP*
  This document is an extension of the Practical ISP and contains details of all the procedures mentioned in the Practical ISP document plus a detailed instructional breakdown of those rules, such as how to do a proper backup. Obviously, the development of such a document can have a significant initial cost in being established. Once it is created it can provide for employee training and consistency. Detailed ISPs can be over 200 pages long.

The names of these different policies may varies from organization to organization, and may be quite different from the above, yet it is easy to classify given document to any of these three groups.

GENERAL ISP

As mentioned before the general ISP is usually very short and outlines the wish of the top management to protect information resources of the organization. Below is an example of such a policy introduced at the University of Auckland, New Zealand (2006):

By proactively managing information security, the University can reduce the likelihood and/or the impact on our information systems from a wide range of threats. These threats include:

- Theft of physical IT assets,
- Theft and exploitation of information,
- Deliberate disclosure of sensitive information by University people, agency or contract employees,

- Accidental disclosure of information by University people, agency or contract employees through careless talk (social engineering) or poor document control,
- Destruction or corruption of information stored on computers whether deliberate or accidental,
- Prosecution because of non-compliance with legislation e.g. the New Zealand Privacy Act,
- Concerted attacks on our networks and information by highly organised and computer literate groups; e.g. hacking, denial of service attacks, worms and viruses.

As it was shown in this example the objective of the General ISP is only to indicate the wish of management to protect their information resources. General ISPs does not say how to do this or what consequences would be imposed on those who do not follow it.

PRACTICAL ISP

This is a publication, which contains a number of headings with short (one or two sentence) blurbs. For instant it could be titled as "The Quick Reference Guide to Information Security" and cover issues such as:

1. Access to Information
2. Password Generation & Control
3. Notebook & Laptop Security
4. Viruses
5. Work From Home, etc

Each entry is summarised by a short instruction. For example (from an original company document) the issue of "Destruction of Computer & Telephony Hardware" was followed by: "Information Services are responsible for computer & telephony hardware assets and will determine the method of disposal for each individual item".

More extended version could be represented by a 50 page long document labelled "Information Security Policy" including such parts as:

- *Scope of the Policy*
  General introduction on what the policy covers, applicability, etc
- *Assets Classification and Control*
  This is one of the most important security policy aspects: the definition of access rights to all of the organization's assets which are not freely available and methods of managing these privileges
- *Personnel Security*
  All measures necessary to have trustworthy staff and methods of verifying this trust.
- *Physical and Environmental Security*
  Every real company uses office space and owns/uses office and ICT equipment. This space/equipment should be protected and that part of the ISP addresses these requirements.
- *Computer and Network Operation and Management*
  All protection measures related to computer hardware/ software and networks. This may include the firewall settings, protection against viruses and SPAMs.

Each chapter outlines specific group policies. For instance the "Personnel Security" chapter could contain several Objectives, followed by Policy and Guidelines like:

- *Objective*
  To minimise the damage from security incidents and malfunctions, monitor and learn from such incidents.
- *Policy*
  Channels for reporting security incidents and malfunctions shall be established and all staff made aware of them.
- *Guidelines*
  Staff should be made aware of the purpose and use of the channels for reporting security incidents

A disciplinary process should be instituted for dealing with security breaches.

The above is a quote from an anonym company document.

In many cases the Practical ISP is printed as a short document and staff are asked to read and follow it. For instance, the University of Auckland Practical ISP (2006) warns the staff and the students: "Users who do not comply with mandatory IT policy will be subject to the provisions of the appropriate statute".

DETAILED ISP

A detailed ISP is an extension of the Practical ISP. Not only does it define what needs to be protected but also states how it could be done. For instance while the practical ISP may imply that each employee should back up files, the detailed ISP would instruct the user on how this should be done. This policy may also define how often this needs to be carried out plus how to retrieve backed up data. Such a document could be well over 200 pages long.

It is obvious that an effort to produce such a document is usually significant and that only large organization can afford to do this. Janczewski and Tai (2006) stated (in relation to the practical ISP within accounting Small and Medium Enterprises, (SME)):

All respondents seem to have an information security policy in their organizations. However, a more careful analysis reveals that what they have might not be a real "information security policy" as some of the respondents said they have "IT policy" (or something to that effect). While IT policy might govern what employees can or cannot do with the IT system, an information security policy should go beyond the IT system and include policies on operational or procedural matters. So even though the respondents have policies in place, the policies might not be of good enough quality.

This implies that in practical terms none of those SMEs developed a detailed ISP.

On the top of the large costs related to producing such a document the maintenance effort spent on it could be equality prohibitive. It is clear that such a policy may only make sense if it is properly updated.

The author of this paper recalls a case of auditing a branch office of an international bank where the branch IT manager produced a copy of their detailed ISP. One of the points there was the definition of a procedure for handling of faulty computer equipment. The regulation stated how to report a fault and prepare the equipment for repair. Further, it was indicated that a specific company is authorized to service the equipment. It looked faultless. But in the meantime the bank had changed the repairer making the name in the ISP not valid. One could imagine the consequences of shipping faulty equipment containing sensitive information to an unauthorized service dealer!

IS STANDARDIZATION OF ISPS POSSIBLE?

There are several, sometime conflicting parameters:

- Companies differ in every possible aspect: domain, objectives, size, and IS technology implemented.
- The business environment is usually based on a LAN-type network spanning desk top machines, mainframes and servers with connection to the outside word. This connection may be of the many types including VPN, dial up, and WEB based.
- The application and system software used could be different, however one element is common: no application is perfectly separated from the rest of the world. Through CD ROMs and USB devices even standalone machines are able to exchange data.
- The law in each country is different and may impose different constraints on a company's information systems in terms of the security of their and other's data and software. However, there is a noticeable world trend to standardise law. A company wishing to benefit from international trade must abide with other country's regulations. This puts pressure on local law to follow other international regulations.

This means that security mechanisms & procedure descriptions must be set up to guard information assets from destruction or unauthorised modification. This forces each company to set up their own data security policies which should have

a common denominator. Is a generic ISP such a common denominator? In the author's opinion the answer is a qualified YES, due to the following reasons:

- Internationally ICT has become highly standardised. The trend is similar to the automobile industry where cars are produced by different companies that look relatively similar but:
  - o They are assembled in many countries and shipped internationally,
  - o Driving methods are practically the same,
  - o Main subassemblies work on the same or similar principles.

  The same applies to the ICT industry.
- The growth of the international trade is significant. Each supplier must be prepared to co-operate with a wide range of customers. This puts pressure to adjust their own structure to that of their customers.
- The production/trade methods around the world have become standardised. During the writing of this paper tensions between the USA and Iran are high. But despite what these two countries represent in terms of the political doctrines or culture models, it is obvious that the ICT equipment used in both countries is more or less compatible and is used in a similar way.

Despite all of these compelling reasons many companies, especially SMEs, have not developed a full ISP set (Tai, 2006). The main reason for this is due to the relatively high demand for financial and human resources to develop and maintain such a set of documents. There should be a way of reducing these costs and the next section explains how this could be possible.

APPROACHES TO ISP DEVELOPMENT

The most elaborate approach to setting up an ISP is to develop it as a part of a waterfall methodology suggested by many authors. One of the best examples of this was presented by Whitman and Mattord (2005). In this case the ISP is a part of the whole process starting at the decision to develop an information security system and concluding with system implementation, maintenance and update. If done correctly, such a procedure would lead to the best results; however the costs would be enormous.

The other approach is to take into consideration the most popular international security standard, the ISO 17799 *Code of practice for information security management* (2005) and use it as a framework to develop a company ISP. This way the quality of the resulting ISP would be very high while the effort would be significantly lower than using the fully sized risk analysis and development process. This was well proved by Tai (2003).

Probably the most robust and quickest way of developing an ISP is to use a *Toolkit*, or a *Toolbox* (von Solms, 2001) developed at the Nelson Mandela Metropolitan University, Port Elisabeth, South Africa (former Port Elisabeth Technikon). The concept of the toolbox is based on using the ISO 17799 standard as a foundation stone of the software package guiding the ISP developers though the process of constructing an ISP document.

The Toolbox is an integrated software driven tool. It is based on a very sound theoretical foundation. However its "intelligence" helps novice security officers in setting up the ISP quickly and efficiently. It also may be used as a support tool for experienced consultants.

Each of the above presented methods has advantages and drawbacks. The first method allows the development of a custom-tailored ISP, which is the best for the given conditions, but the cost would be substantial. On the other hand, the last approach allows the quick development of a basic (yet practical) ISP.

Many authors have presented examples of ISP, such as Janczewski & Colarik (2004) or comprehensive instruction how to setup an ISP (Kaon, 2006).

NEGLECTED ISP ISSUES

A well developed ISP contains sections addressing issues such as:

- Organization of Information Security
- Asset management
- Human Resources Security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

This list makes up the foundation of the ISO 17799 standard.

Regulations are required for the areas addressed in the list above. However, some of these issues are not receiving proper attention and may result in significant security breaches and considerable losses. The issue that will be addressed in this paper is the issue of the ownership of documents or files and authorised access to them.

Almost all security models define security levels and categories. The lattice theory is based on this (Amoroso, 1994). The introductory step in there is definition of possible security levels and categories. In a military institution such a listing may look as it is presented in the Table 1.

Table 1. Example of security levels and security categories

Security levels		Security category
Top secret		HQ
Secret		Navy
Confidential		Army
Limited circulation		Air forces
No restriction		

It is possible for the number of security levels to differ from the number of security categories. Also, it is not important (apart from the psychological point of view) what terms are used to name each of the security levels. The security categories are usually associated with different units of an organization.

Now, a number of interesting questions should be made:

- How many security levels are needed?
- How strictly should we determine the borders between these levels?
- Are the assigned levels and categories strict or can they change over time?

The number of security levels must have an optimum. One security level does not make any sense. This would imply that all the documents are available to anybody and few would follow this principle. Therefore two levels is an obvious minimum but may not provide proper protection of information. On the other extreme, many security levels, like, say 20 or 30 does not make sense as this would make it impossible to manage such a system.

All this implies is that any organization embarking on the introduction of a security classification system must decide how many levels should be generated. In saying that there are limitations:

- The initial most obvious choice is the introduction of 3 levels, which could be labelled as:
  - o No restriction (the document is accessible for anybody)
  - o Internal use (the document is accessible for employees only)
  - o Confidential (the document is accessible to a restricted number of employees)
- In military and governments usually there are at least 4 security levels: "general", "internal circulation only", "confidential", and "top secret". The "top secret" is for use by a limited number senior management.

Generally speaking the choice of the number of security levels is a function of two variables:

- The security needs of the organization (more security levels allow the better tailoring of security systems to the desired needs).
- The economy of the system (more security levels cost more to implement and maintain)

The next issue is the strictness of the division between security levels. Janczewski & Portougal (2000) studied this specific issue. They came to the conclusion that it is worth making the borders fuzzy. Sometimes shifting an item up or down the confidentiality scale could have noticeable economic effects.

Table 2. Standard security label

Security level	Security category
Secret	Human resources

Table 3. Improved format of a security label

Security level	Security category	Expire date	Owner
Secret	Human resources	12 March 2008	Smith

Starting from the Bell LaPadula security model (1973) through the Orange Book (1985) and culminating on the previously mentioned ISO standard 17799, all sources advocate the development of security labels attached to all subjects and objects. The security label is a record of the security level and security category of the object to which is attached. One should note that the security category is sometimes referred to as the "security compartment". A security label could look similar to this in the Table 2.

An obvious question must follow: is such a security label adequate for a typical business environment?

Imagine the following situation: A company is preparing a marketing plan and the plan is considered as a top secret and a *top secret* security level is attached to it. The CEO of the company then appears on national TV and announces the new marketing strategy. What would you think reading such a document later seeing the "Top security" label still attached to the document?

The other important aspect of the label is that what should be done if changes are made to the document?

The obvious solution to this problem is to nominate a person as an owner of the document and authorise only this person to introduce changes to it. These changes could relate not only to the content of the document itself but to the content of the label.

Hence, it seems sensible that a security label of any document or file should have a format presented in the Table 3.

This security label was extended to include fields describing the date of the document expiring and an indicator of who the owner is. Such a label has significant advantages especially in the case of electronics processing. A system validating all the classified documents would inform the owner of a document about it's expiry date and ask for a decision on what to do next with the content of the security labels and the document itself. As a result an appropriate change could be done such as like removing it from circulation or changing its security level.

CONCLUSION

All the above allows us to formulate the following conclusions related to the ISPs:

1. Each company should develop a set of documents relating to Information Security management that includes a brief guide, full policies and detailed procedures. Emphasis should be placed on the full policy (or the Practical ISP).
2. These documents should contain a set of major clauses regarding such issues as assets classification and control, personnel security, physical security, computer operations, network operations, system access control, and risk management.
3. The development of an ISP could be the result of a full risk analysis but without noticeable decrease of the quality of the final document other methods offer similar products with significant costs and time reduction.
4. A generic ISP documents forms the foundations stone of these methods.
5. Development of a good ISP should be preceded by establishing rules of handling sensitive information/documents, such as the establishment of the security levels and the handling limited circulation information. One can imagine the confusion resulting from the introduction of security labels within an organization which did not set before these rules before.

Hence future research should be aimed at developing a methodology of evaluation of company information systems from a security point of view. Such evaluations could include the analysis of:

- Procedures of handling company customers and suppliers,
- Structure of the telecommunication system
- Internal flow of information, etc.

REFERENCES

Amoroso, E., Fundamentals of Computer Security Technology, Prentice Hall, 1994

Anderson, R., Security Engineering, Wiley, 2001

Bell, D., LaPadula, L., Secure Computer Systems: Mathematical Foundations ESD-TR-73-278, Vol1, Mitre Corporation, 1973

DPMA Model Corporate Computer Security Policy Statement, quoted after: DPMA Model Corporate Computer Security Policy Statement, http://accounting.uwaterloo.ca/ccag2001/6CHAP97.htm, reviewed 2006

Forch, K., Computer Security Management, Boyd & Fraser, 1994

The Generally Accepted Information Security Principles, http://www.issa.org/gaisp/_pdfs/overview.pdf, reviewed 2006

ISO 17799 Code of practice for information security management, ISO, Second edition, 2005,

Janczewski, L., Colarik, A., A Managerial Guide to Cyberterrorism and Information Warfare, IDEA Publishers, 2003

Janczewski, L., Tai, V., Security Status and Model for Mid-size Accounting Firms in New Zealand, Proceeding of the 2006 IRMA International Conference, May, 2006

Janczewski, L., Portougal, V., „Need-to-know" principle and fuzzy security clearance modelling, Information management & Computer Security, No 5, 2000

Kaon Technologies, Information Security Policy, http://www.kaonsecurity.com/html_pages/policy_main.htm, reviewed 2006

National Computer Security Center Department of Defence Trusted Computer Security Evaluation Criteria, DoD 5200.28-STD, 1985

Tai, V., Development of Information Security Policy with use of Information Security Standards", A research essay, The University of Auckland, January 2003

Whitman, M., Mattord, H., Principles of Information Technology, , Thomson, Second Edition, 2005

The University of Auckland: Why do we need to manage information security?, http://www.auckland.ac.nz/security/FAQ.htm, reviewed 2006

The University of Auckland, Compliance with policy, reviewed 2006, http://www.auckland.ac.nz/security/compliance.htm

Von Solms at all, The Information Security Management Toolbox, Proceedings of the 1st Annual Information Security for South Africa Conference, ISSA2001, 2001